The cloud is becoming a major computing environment. Many critical applications are being migrated to cloud platforms. These include medical and finance applications, big data applications, and applications with real-time constraints. Gartner predicts that the bulk of future IT infrastructure spending will be on cloud platforms and applications, and nearly half of all large enterprises are planning cloud deployments by the end of 2017.

However, cloud computing systems and services have become major targets for cyberattackers. Because the cloud infrastructure is to a certain degree an open and shared platform, it’s subject to malicious attacks from both insiders and outsiders. The high degree of virtualization in cloud systems also makes them ideal subjects for side-channel attacks. Identity hijacking and distribution of malicious code have become critical issues in cloud systems. Thus, organizations must carefully plan, deploy, and maintain centralized management of security properties and effectively enforce security policies in cloud environments.

To provide strong protection of cloud platforms, infrastructure, hosted applications, and data stored in the cloud, we need to address the security issue from a range of perspectives. These include secure data and application outsourcing, information leakage protection, information retrieval on encrypted data, anonymous communication, vulnerability discovery, attack handling, homomorphic encryption, and secure multiparty computation. To achieve the high level of cloud security management required, we need comprehensive vulnerability analyses and innovative security technologies in both theory and practice.
The Articles

By organizing this special issue on cloud security, it was our intention and hope to emphasize and address the importance of protecting and securing cloud platforms, infrastructures, hosted applications, and data storage.

We received 42 submissions in response to our call for papers. After two rounds of rigorous review, we selected five high-quality papers for publication in this special issue.

In "Online Analysis of Security Risks in Elastic Cloud Applications," Athanasios Naskos, Anastasios Gounaris, Haralambo Mouratidis, and Panagiotis Katsaros address security-related concerns in elastic cloud applications stemming from the inherent tradeoffs between security and other non-functional requirements, such as performance. To this end, the authors propose a solution that can be efficiently realized by modeling the application behavior as a Markov decision process, on top of which they apply probabilistic model checking. The authors show how their approach can be used to perform online analysis and elastic decision making, and how its runtime analysis can provide evidence for key security-related aspects of the running applications, such as determining the probability of data leakage in the next hour.

In "Privacy-Preserving Access to Big Data in the Cloud," Peng Li, Song Guo, Toshiaki Miyazaki, Miao Xie, Jiankun Hu, and Weihua Zhuang focus on the security and privacy concerns regarding third-party cloud storage service providers, which cause many users and companies to hesitate to move their data to cloud storage. The authors provide a tutorial and survey of oblivious RAM (ORAM), a solution designed to enable privacy-preserving access to data stored in the cloud. Moreover, the authors study the access load balancing problem when applying ORAM for big data in the cloud, and propose heuristic algorithms to achieve access load balancing in both static and dynamic deployments.

In "Cryptographic Public Verification of Data Integrity for Cloud Storage Systems," Yuan Zhang, Chunxiang Xu, Hongwei Li, and Xiaohui Liang also deal with the security of cloud storage services but from a different angle: the verification of data integrity. Many public verification schemes employ a third-party auditor to verify the integrity of data outsourced to cloud storage services, but they’re effective only if a strong assumption holds: that the auditors are honest and reliable. Moreover, many such schemes are vulnerable to an active external adversary, who can modify the outsourced data and tamper with the interaction messages between the cloud server and the auditor. The authors propose an efficient and secure public verification scheme that uses a random masking technique to protect against external adversaries, and requires users to audit auditors’ behaviors to prevent malicious auditors from forging verification results. The authors also use Bitcoin to construct unbiased challenge messages to thwart collusion between malicious auditors and cloud servers.

In "To Docker or Not to Docker: A Security Perspective," Theo Combe, Antony Martin, and Roberto Di Pietro address the security of cloud-based infrastructures. They first provide a comprehensive overview of the container ecosystem, which was designed for shortening development cycles, providing continuous delivery, and achieving cost savings in cloud-based infrastructures. The remainder of the article is dedicated to the introduction of Docker, which is both a leading container solution and a complete packaging and software delivery tool. Using realistic use cases, the authors discuss the security implications of the Docker environment. Moreover, they define an adversary model, point out several vulnerabilities affecting current Docker uses, and discuss future research directions for Docker.

In "User-Centric Security and Dependability in the Clouds of Clouds," Marc Lacoste, Markus Miettinen, Nuno Neves, Fernando M.V. Ramos, Marko Vukolić, Fabien Charmet, Reda Yaich, Krzysztof Oborzyński, Gitesh Vernekar, and Paulo Sousa consider the issue of lack of interoperability in a distributed environment of multiple clouds, and point out that the complexity of management could raise many security and dependability concerns. The authors introduce secure Supercloud computing as a new paradigm for security and dependability management of distributed clouds. Supercloud follows a user-centric and self-managed approach to avoid technology and vendor lock-ins. In this system, users can define U-clouds, which are isolated sets of computation, data, and networking services run over
both private and public clouds operated by multiple providers, with customized security requirements as well as self-management for reducing administration complexity. The authors present the Supercloud security architecture along with several use cases to illustrate its practical applicability.

We hope you enjoy reading these five articles and expect that the publication of this special issue will both increase public awareness of the significance of cloud security and inspire further investigation on the development and enhancement of state-of-the-art cloud security solutions.

PETER MUELLER is a research staff member at IBM Research. His research interests include datacenter storage security and reliability and high-frequency technology. He's a senior member of IEEE and a member of the Society for Industrial and Applied Mathematics, the Electrochemical Society, and the Swiss Physical Society. Contact him at pmu@zurich.ibm.com.

CHIN-TSER HUANG is an associate professor of computer science and engineering at the University of South Carolina, where he's the director of the Secure Protocol Implementation and Development Laboratory. His research interests include network security, network protocol design and verification, and distributed systems. Huang has a PhD in computer science from the University of Texas at Austin. He's a senior member of IEEE and ACM, and a member of Sigma Xi and Upsilon Pi Epsilon. Contact him at huangct@cse.sc.edu.

SHUI YU is a senior lecturer in the School of Information Technology at Deakin University, Australia. His research interests include networking theory, network security, privacy and forensics, and mathematical modeling. He's a senior member of IEEE. Contact him at shui.yu@deakin.edu.au.

ZAHIR TARI is a full professor of distributed systems at RMIT University, Australia. His research interests include system performance (for example, web servers, peer to peer, and cloud computing) and system security (such as SCADA systems and the cloud). Tari has a PhD in computer science from the University of Grenoble, France. Contact him at zahir.tari@rmit.edu.au.

YING-DAR LIN is a distinguished professor of computer science at National Chiao Tung University, Taiwan. His research interests include design, analysis, implementation, and benchmarking of network protocols and algorithms, quality of services, network security, deep packet inspection, wireless communications, embedded hardware/software co-design, and software-defined networking. Lin has a PhD in computer science from the University of California, Los Angeles. Contact him at ydlin@cs.nctu.edu.tw.

CONFERENCES in the Palm of Your Hand

Let your attendees have:
• conference schedule
• conference information
• paper listings
• and more

The conference program mobile app works for Android devices, iPhone, iPad, and the Kindle Fire.

For more information please contact Conference Publishing Services (CPS) at cps@computer.org

myCS Read your subscriptions through the myCS publications portal at http://mycs.computer.org.